

## SS理数数学 I 課題学習 (情報交換しながら記入せよ。スマホ可)

<フェルマーの小定理 (Fermat's little theorem) >

$p$  が素数,  $a$  が任意の自然数のとき

$$a^p \equiv a \pmod{p}$$

特に,  $a$  と  $p$  が互いに素な自然数のとき

$$a^{p-1} \equiv 1 \pmod{p}$$

フェルマー (Pierre de Fermat)

17世紀  の数学者。「フェルマーの  定理」 ( $n \geq 3$  である自然数  $n$  に対して,  $x^n + y^n = z^n$  は自明でない整数解を持たない) は, 360年の長きにわたり未解決問題として有名であった。(1995年,  が証明完成。)

**課題 1** 具体的な数でフェルマーの小定理が成り立つことを確認せよ。

例 1 :  $p=3$ ,  $a=4$  のとき,  $4^3 \equiv 64 \equiv 1 \pmod{3}$

$$4 \equiv 1 \pmod{3} \quad \therefore 4^3 \equiv 4 \pmod{3}$$

$$\text{また } 4^{3-1} \equiv 4^2 \equiv 16 \equiv 1 \pmod{3}$$

他の例を 3 つ書け

**例**  $7^{100}$  を 11 で割った余りを求めよ。

フェルマーの小定理より、

$$7^{10} \equiv 1 \pmod{11}$$

これより、

$$7^{100} \equiv (7^{10})^{10} \equiv 1^{10} \equiv 1 \pmod{11}$$

であるから、 $7^{100}$  を 11 で割った余りは 1 である。

**課題 2** フェルマーの小定理を用いて答えよ。

(1)  $3^{1000}$  を 7 で割った余りを求めよ。

(2)  $5^{1000}$  を 13 で割った余りを求めよ。

<フェルマーテスト>

フェルマーの小定理を書き直すと

$$p \text{ が素数} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

フェルマーの小定理の対偶を書くと

$a$  と  $p$  が互いに素な自然数のとき

$$a^{p-1} \equiv 1 \pmod{p} \text{ にならない} \Rightarrow p \text{ は合成数。}$$

**課題 3** 91 は素数か合成数か。フェルマーの小定理の対偶を用いて答えよ。